

# Master Windows XP firewall

If you have Windows XP, you have some useful firewall protection at your fingertips. Karl Wright explains how to get the best from this security tool and avoid any conflicts

In this article, we will look at the protection provided by the Windows firewall and how you can ensure it gives the best security possible without causing problems elsewhere in your system. First, you need to make sure the firewall is switched on; see the screens below. Once you've done this, there are a few simple things you can do to make sure that while your system is protected, the firewall doesn't interfere with the proper working of any legitimate software.

If you have installed Service Pack 2 (SP2) for Windows XP, the firewall will be switched on by default. If you have a third-party firewall program installed, it will disable the Windows firewall. That's fine while it's installed, but if you uninstall it, check to make sure that it has switched Windows XP's firewall back on.

## MAKING EXCEPTIONS

The Windows firewall doesn't monitor traffic leaving your PC, so any program on your PC can transmit data to the internet. This means that web browsers can send requests to websites and email programs can connect to email servers.

Some software is designed to send data to the internet in response to a request sent to it from a remote computer. The default behaviour of the firewall

is to block this initial request, because you don't usually want your PC to respond to unsolicited connections from the internet. However, this makes some programs on your PC stop working.

Many networked games behave in this way, and with the firewall running with its default settings, you won't be able to play against other networked gamers. To get around this, you must tell the firewall to make an exception for the program in question as shown in the walkthrough above right. When an exception is set up, the firewall selectively opens the relevant ports to allow incoming connections to the excepted program alone.

Creating an exception isn't risk-free. Open ports provide attackers with opportunities to meddle with your PC and they may sometimes be able to gain entry to your system; see the box called 'Who's listening?' over the page. If you use a dial-up connection, there's even a chance you could make all your shared files available over the internet, though thankfully Microsoft has released a fix for this. You can find it at <http://support.microsoft.com/kb/886185>.

In some situations, you may feel your PC is particularly vulnerable. Maybe you have connected your notebook to a public network in an airport or hotel, for instance. In this case, you can tick the 'Don't allow exceptions' box. This inactivates all your exceptions, and they remain inactive until you untick the box. Use this mode only when you really have to, because it also disables things such as file and printer sharing, severely restricting what you can do with your PC.

## ADDING A PORT

If a program still doesn't work, even when it has been listed as an exception, you can try adding the TCP or UDP ports that this program uses to the list of exceptions. We recommend this only as a last resort. If you except a port rather than just a program, someone could connect to any program on your PC that is listening on that port. This could include a virus or remote control Trojan.

Moreover, some programs may change the port they use or use a range of ports. In this case, you'll have to add each port separately, which is a real pain. If you really have to open a port, however, see the walkthrough below right for how to do it. To find out which ports a program uses, consult its manual or the developer's website. If the program communicates only with specific computers, limit the use of that port to those computers, either by stipulating that only PCs on your home network can use the port or by specifying the IP addresses from which communications will be accepted. Take a look at the walkthrough for details.

You can also limit programs that you've listed as exceptions in the same way. Some applications only work, or work much better, when specific ports have been opened. BitTorrent clients, for instance, use TCP port 6881-6889. Opening these ports gives you much faster download speeds. Some games also require you

## INTRODUCTION

An anti-virus program alone isn't enough to keep your PC safe; you need a firewall, too. A firewall is a piece of software or hardware that monitors the traffic between your PC and the internet, and stops any communication that looks suspicious. Fortunately, Windows XP comes with its own firewall, and from Service Pack 2 this is enabled by default. It looks very simple, but it offers powerful security with lots of useful features. In this article we show you how to get the most out of it.

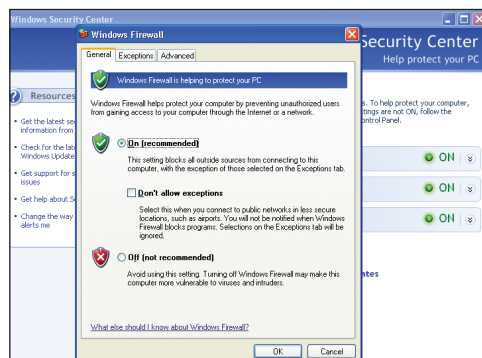
**Karl Wright**  
Systems engineer  
and IT journalist



windows@computersshopper.co.uk



▲ From the Start menu, go to Settings and open the Control Panel. Click on the icon called Security Center. If Control Panel is set to Classic View, just click Firewall

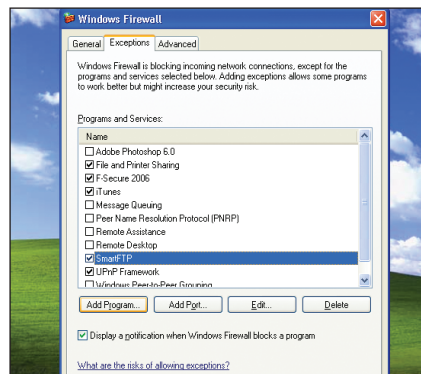


▲ Click on Firewall. In the window that pops up, make sure Firewall is ticked, but that the box marked 'Don't allow exceptions' isn't

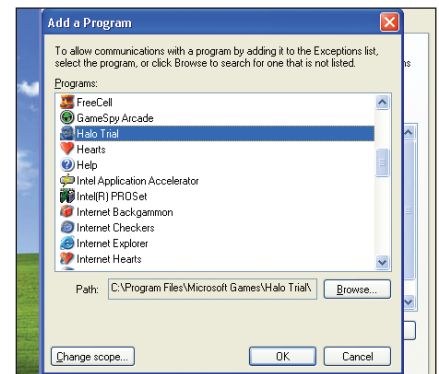
# HOW TO... Create an exception



**1** Open the Windows firewall and check the first tab to make sure exceptions are allowed. Then go to the second tab, which is called Exceptions. Here you'll find a list of all the programs and services that are currently excepted



**2** We want to allow a multiplayer game called Halo to work, but it isn't on the list of exceptions. Click Add Program and check the second list of programs that appears. It's not there, so click on the button called Add Program



**3** Search the list of programs until you find the one you want, then select it and click OK. If the program isn't on the list, click Browse and manually find and select the program's executable file. It will be in the Program Files directory

to open specific ports if you want to play against other gamers over a network. To play Call of Duty 2 over a network, for instance, requires you to open TCP port 28960.

## ADVANCED FUNCTIONS

If you open the Windows firewall from Control Panel, you'll see the third tab is called Advanced. This contains several functions that are worth exploring. The first and most straightforward is the Network Connection Settings box. All your network adaptors are listed in this box. By ticking or unticking the box next to each one, you can choose whether or not you want that connection to be protected with the firewall.

This is useful if you connect to the internet through one adaptor but to a trusted network on another. If you select an adaptor and click on its Settings, you can choose which services you run on your PC that you want to be available to other systems over the network. For instance, if you're running the Internet Information Service (IIS) web server and you want your PC to act as a web server for other computers on the network, you'll need to tick Web Server (HTTP) on this list.

The third section on the Advanced tab is called ICMP, which stands for Internet Control

Message Protocol. If you click on the button marked Settings, you'll see a list of options. All but one of these (Allow incoming echo request) will be disabled. These options determine what information your PC will give out about itself when it is asked. If you enable these settings, you will be able to use the command prompt on any one of your networked PCs to interrogate any other.

We recommend that you leave them unticked for security reasons. Enabled, these settings can allow an attacker to discover information about your network. As long as your network isn't large, you can enable these settings in a few minutes if and when you need them. Leave the Echo Request option ticked. This can be a very useful utility for diagnosing quickly where a network problem lies, allowing other PCs to ping the computer to see if it's running.

## FIREWALL LOGS

Windows Firewall doesn't alert you to every single intrusion attempt, but it does keep a detailed log in which it records all attempts to gain access to your computer. In order to view the log file, you need to browse to the C:\Windows directory and open the file

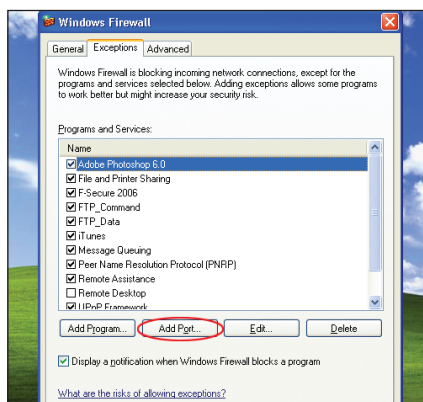
pfirewall.log in Notepad. You'll see lots of entries that look something like this:

```
2006-03-12 02:58:52 OPEN TCP 192.168.1.2
207.46.18.30 4927 80 - - - - -
```

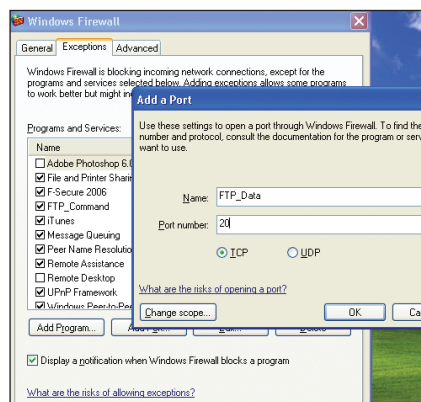
The first three sets of numbers are the date (yyyy-mm-dd) and the second set of numbers are the time. Open TCP refers to the action the firewall has taken, in this case to open a TCP port. If it had blocked an unauthorised connection, it would read DROP TCP instead. The number 192.168.1.2 is the PC's own IP address, while 207.46.18.30 is the IP address of the remote PC to which we were trying to connect. The numbers 4927 and 80 are the source and destination ports respectively; the ports that were opened for the communication. Port 80 is the standard port for web servers.

If you suspect you're being hacked or have been infected by some malware, this information can be a lifesaver. You could look down the list for repeated attempts to access ports from a particular IP address, or you could identify that there have been attempts to make connections to the internet. In that case, use the netstat -b command to find which program is making the

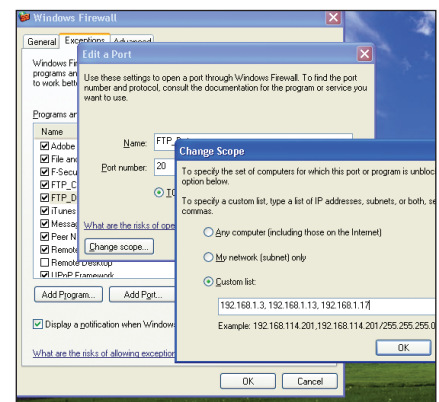
# HOW TO... Open a port



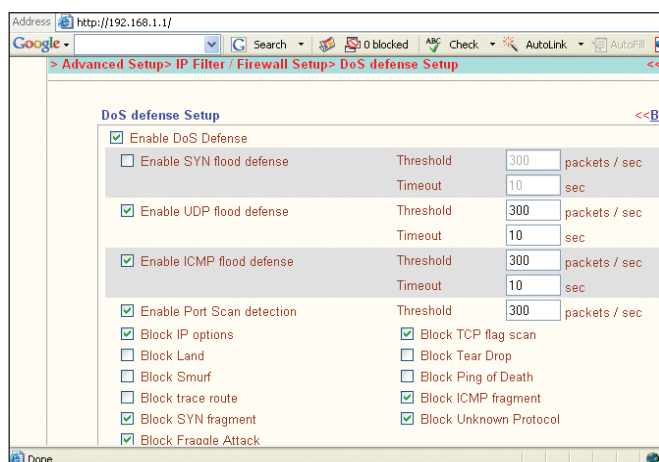
**1** Open Windows XP Firewall's Exceptions tab and click on the Add port button. This button will open a form that contains two empty boxes



**2** Provide a name for the exception and specify whether you're opening a TCP or UDP port. Type the port number into the bottom box



**3** Click on the Change scope button and specify whether you want any PC to be able to use this port, only PCs on your home network, or only PCs with specified IP addresses



◀ This is the control panel of a hardware router. Everything you need to secure your network is here, but you'll need to know what you're doing when you set it up

attempts (see box opposite). Then run your anti-virus software and make sure it scans the program that netstat reports. If it fails to detect a virus, at least you have some useful information to give to your anti-virus vendor. The vendor may then be able to help you clean your system.

## LIMITATIONS

Compared to certain third-party products, Windows XP's firewall suffers from a few important limitations. You can't specify that a range of IP addresses, say from 192.168.1.2 to 192.168.1.10, should be trusted to communicate over a particular port. Instead, you have to specify each individual address in the range.

As we've already mentioned, the Windows XP firewall can be turned off by other applications, most commonly third-party firewalls that don't want it running in the background. Unfortunately, what's true for third-party firewalls is also true for certain malware. The Bagle virus, for example, switches off the Windows firewall so hackers can break into your PC. There is an easy solution, though. Simply ensure you have a good, up-to-date virus scanner. Of course, it would be better if the firewall wasn't quite so easy to turn off.

The Windows XP firewall doesn't monitor outbound traffic at all; only inbound data packets are checked. Many malicious programs, viruses and spyware are designed to transmit information about your PC and its contents over the internet. Third-party firewall programs protect against this, but the Windows XP firewall does not.

## EXTRA HELP

If you decide that the Windows firewall doesn't offer you enough protection, you have a couple of options. You could choose to use another software firewall such as ZoneAlarm, which is available as a free download from [www.zonelabs.com](http://www.zonelabs.com). This has all the features of

Windows XP Firewall and monitors outbound traffic. It lets you specify a range of IP addresses as blocked or allowed, too.

ZoneAlarm has far more sophisticated and specific filter and blocking features. These give dedicated users, who are prepared to spend some time and effort configuring settings, far greater control over which programs can send data in and out of the PC, and on which ports. If you do decide to install another firewall program, make sure that it switches Windows' firewall off. Running two software firewalls on the same PC may cause conflicts that will stop some programs working.

If this doesn't satisfy you, you could opt for a hardware firewall instead (or as well). A hardware firewall is a box that stands between your network and the internet. It monitors all the traffic that passes through it and blocks anything that it regards as illegitimate, depending on the rules you've set.

There are many advantages to having a hardware firewall. It's far more difficult for a piece of malware such as a virus to tamper with its settings, for a start. A hardware firewall does not impose any strain on your PC, unlike a piece of software that has to be run constantly in the background. It will protect every PC on your network, too, regardless of which operating systems are running.

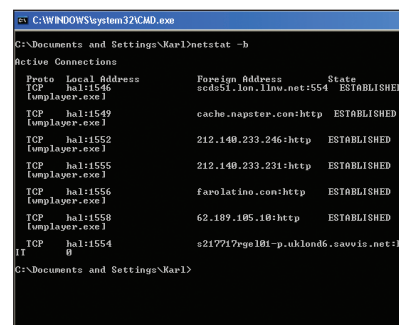
Many home users won't want to spend money on a dedicated piece of security hardware, but it's not as expensive as you might think. Most broadband routers have them built in already. If you use a hardware firewall as well as software firewalls on networked PCs, make sure any ports you need to be open are opened on both the hardware firewall and the PC running the service. You may have to find out which ports are used by any programs you've listed in the Windows Firewall Exceptions list and open those ports manually on your hardware firewall. **CS**

## Who's listening?

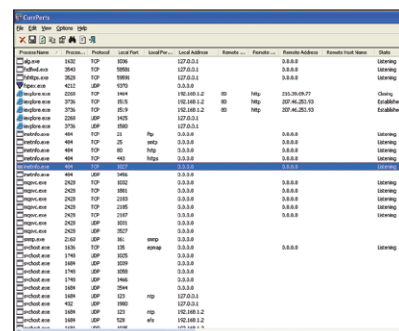
If there is malware on your system, it will probably listen on a port, waiting for a communication from its master that will prompt it to start transmitting information about your PC. If you think this might be the case, you can check using a tool called netstat, which is built into Windows XP.

From the Start menu go to the Run box and type cmd. At the command prompt, type netstat -b. This lists all the network ports that are being used or listened to, as well as the program that is using or listening to each. If you spot something suspicious, you should make sure neither the executable nor the port it is using is on the firewall's list of Exceptions. Then update your anti-virus and anti-spyware programs and scan your entire PC.

If you don't fancy fiddling about with the command line, you could simply download the excellent CurrPorts from [www.nirsoft.net](http://www.nirsoft.net). This shows all the processes connected to the network and all those currently listening for connections to be initiated, in an easy-to-understand graphical user interface.



▲ Netstat shows you all the ports currently being used to connect to the internet and lists the executable file connected to each port



▲ CurrPorts does the same as netstat but is much easier to understand because of its Windows interface

## What's a port?

To communicate with each other, all the devices on a network must speak the same language. For PC networks, this language is usually TCP/IP. Each PC on a TCP/IP network has to be uniquely identifiable. One unique identifier is the PC's MAC address, which is a unique serial number hard-coded into the network card. But at the software level, IP addresses are used to identify a system.

A computer can run more than one service. For example, one single computer could be running a web server, a POP3 email server and an FTP server. Let's assume this computer has the IP address of 192.168.1.1. But when you visit this server, how do you tell it that you want to collect your email as opposed to downloading a file over FTP or browsing a web page? Ports come to the rescue. If you contact

192.168.1.1 on port 80, it knows you want its web services. Email is provided using port 110 and the FTP server runs on port 21. There are 65,535 permitted port numbers, many of which have been standardised. That's not to say you can't break the rules. While it would be normal to run a web server on port 80, you could run it on port 81, port 8,000 or any other number between 1 and 65,535.